



# UNITED STATES PATENT AND TRADEMARK OFFICE

*Handwritten signature/initials*

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,493	07/06/2001	Michael Freed	NEXSI-01111US0	4137
28863	7590	08/11/2006	EXAMINER	
SHUMAKER & SIEFFERT, P. A. 8425 SEASONS PARKWAY SUITE 105 ST. PAUL, MN 55125			LAFORGIA, CHRISTIAN A	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 08/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/900,493

Applicant(s)

FREED ET AL.

Examiner

Christian La Forgia

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 26 May 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1,2,4,9 and 12-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1,2,4,9 and 12-20 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                                   | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)               | Paper No(s)/Mail Date. _____  |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>5/24/06</u> .   | 6) <input type="checkbox"/> Other: _____                                    |

### DETAILED ACTION

1. The amendment of 26 May 2006 has been noted and made of record.
2. Claims 1, 2, 4-9 and 12-20 have been presented for examination.

### *Response to Arguments*

3. Applicant's arguments filed 26 May 2006 have been fully considered but they are not persuasive.
4. With respect to the Applicant's allegation that Jardin does not teach any manipulation or use of data with respect to a security record, the Examiner directs the Applicant's attention to MPEP § 2131, in particular the discussion of *ipsissimis verbis*. *Ipsissimis verbis* states that the elements of the invention must be arranged as required by the claim regardless of the identity of terminology. In other words, the fact that Jardin does not use the same terminology as the Applicant, yet teaches the elements of the claim language is not enough to distinguish the instant application over the prior art.
5. The Examiner would like to point out that where applicant acts as his or her own lexicographer to specifically define a term, the written description must clearly define the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so redefine that claim term. *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The Applicant fails to meet the requirements of defining a term as set forth in the MPEP § 2106. In order to define a term, the Applicant must do so "with reasonable clarity, deliberateness, and precision" and must "set out his uncommon definition in some manner within the patent disclosure" so as to give one of ordinary skill in the art notice of the change" in meaning. The

Art Unit: 2131

Applicant fails to clearly, deliberately and precisely define the term security record. The Applicant also fails to set out the uncommon definition in the instant application's disclosure.

6. With respect to the Applicant's argument that Jardin fails to teach "security record," the Examiner respectfully disagrees with the Applicant's assertion. The Examiner has interpreted the term "security record" with regard to its broadest reasonable interpretation as a security session that spans multiple packets. The cited sections of Jardin disclose sending and receiving multiple data packets over a secure communication session. As such Jardin discloses a security record spanning multiple packets.

7. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies, such as SSL, are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

8. In response to the Applicant's arguments that Jardin does not suggest that the server does not provide a secure communications with the client, for example using SSL, the Examiner disagrees. Jardin is directed to using SSL to establish a secure link as noted in at least the Abstract, as well as column 4, lines 24-47.

9. In response to the Applicant's arguments that Jardin does not disclose forwarding decrypted, unauthenticated application data to the server, the Examiner disagrees. Jardin discloses redirecting decrypted packets to the server for fulfillment in column 7, line 4, as well as column 7, lines 39-56 and column 8, lines 1-17 and lines 27-41. Jardin discloses that the server broker decrypts the packets and forwards them to the server for fulfillment (i.e. authentication).

Art Unit: 2131

10. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

11. In response to the Applicant's arguments that Lockhart fails to disclose discarding a portion of the decrypted packet, the Examiner disagrees. As shown above, Jardin discloses forwarding the decrypted, unauthenticated packet to the server. As disclosed specifically in column 5, lines 34-36, Lockhart discloses removing a portion of the decrypted data packet. Therefore, the combination of Jardin and Lockhart disclose the claim limitation of discarding a portion of the decrypted unauthenticated packet data.

12. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies, such as discarding the entire packet, are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). As it stands, the claim limitations recite removing only a portion of the data, and not the entire packet as argued on page 6 of the Applicant's response of 26 May 2006.

13. See further rejections that follow.

***Claim Rejections - 35 USC § 103***

14. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Art Unit: 2131

15. Claims 1, 2, 4, 5, 7-9, 12, 13, and 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,681,327 to Jardin, hereinafter Jardin, in view of U.S. Patent No. 5,841,873 to Lockhart et al., hereinafter Lockhart.

16. As per claims 1, Jardin discloses a method for enabling secure communication between a client on an open network and a server apparatus on a secure network (Figure 1 [block 100]), the method performed on a intermediary apparatus coupled to the secure network and the open network (Figure 1 [block 120]), comprising:

negotiating a secure communications session with the client apparatus via the open network (Figure 2 [blocks 210, 220, 230, 240], describes the "handshake" between the client and the server which used to start any communication between the server and the client);

negotiating an open communications session with the server via the secure network (column 6, lines 40-46);

receiving encrypted packet application data for a security record spanning multiple data packets, wherein the security record has a length greater than a packet length associated with the multiple data packet (column 6, lines 65-69)

decrypting the encrypted packet application data in each data packet (column 6, line 67);

forwarding decrypted, unauthenticated application data to the server via the secure network (column 7, line 4).

17. Jardin doesn't teach discarding at least a portion of the decrypted unauthenticated packet application data for the security record prior to receiving a final packet of the security record and authenticating the data.

Art Unit: 2131

18. Lockhart discloses discarding at least a portion of the decrypted unauthenticated packet application data for the security record prior to receiving a final packet of the security record and authenticating the data (column 5, lines 33-65).

19. It would have been obvious to one ordinary skilled in the art at the time the invention was made to discard at least a portion of the decrypted unauthenticated packet application data for the security record prior to receiving a final packet of the security record and authenticating the data, since Lockhart states at column 5, lines 47-65 that such a modification would detect decryption errors in an encrypted data packet, thereby detecting if the packet may have been tampered with.

20. Regarding claim 2, Jardin system discloses forwarding data which spans over multiple TCP segments (column 7, lines 44-45).

21. Regarding claims 4 and 12, Jardin system discloses wherein a remaining portion of the packet application data for the security record is buffered as a minimal length sufficient to complete a block cipher used to encrypt the data (column 2, lines 65 to column 3, line 3). This has been known in the art for quite some time and is support by U.S. Patent Nos. 6,101,543 (column 10, lines 58-67) and 5,825,890 (column 17, lines 21-40).

22. Regarding claims 5 and 19, Jardin discloses the use of TCP/IP. The Examiner holds that authenticating could only take place once the final segment was received, if it were fragmented since **Internetworking with TCP/IP**, by Douglas Comer (hereinafter Comer), states that if any fragments are missing the datagram cannot be reassembled on page 105.

23. As per claim 7, Jardin discloses a method for processing encrypted data transferred between a first system and a second system, comprising:

providing an accelerator device including a decryption engine in communication with the first system via an open network and the second system via a secure network (Figure 1 [block 120])

receiving encrypted data from the first system via the open network in the form of application data spanning multiple packets, wherein a last packet of the multiple packets includes information for authenticating the application data (column 6, line 67);

decrypting the application data contained within the multiple packets as the multiple packets are received (column 7, lines 39-41);

forwarding the decrypted application data as the multiple packets are decrypted to the second device via the secure network (column 7, line 4);

authenticating the application data when the information for authenticating the application data is received in the last of the multiple packets.

24. Jardin does not disclose buffering a portion of the decrypted application data and discarding a remaining portion prior to authentication of the application data.

25. Lockhart discloses buffering a portion of the decrypted application data and discarding a remaining portion prior to authentication of the application data (column 3, line 64 to column 4, line 17, column 5, lines 33-65).

26. It would have been obvious to one ordinary skilled in the art at the time the invention was made to discard at least a portion of the decrypted unauthenticated packet application data for the



Art Unit: 2131

security record prior to receiving a final packet of the security record and authenticating the data, since Lockhart states at column 5, lines 47-65 that such a modification would detect decryption errors in an encrypted data packet, thereby detecting if the packet may have been tampered with.

27. Regarding claim 8, Jardin system teaches wherein receiving comprises receiving SSL encrypted data (column 4, lines 11-12).

28. Regarding claims 9, 13, 17, and 18, Jardin system teaches application data encrypted using SSL, DES, and a 3DES algorithm (column 5, lines 16-20).

29. As per claim 16, Jardin teaches a method of providing secure communications using limited buffer memory in a processing device (column 6, lines 5-11), comprising:

receiving encrypted data having a length greater than a TCP segment carrying said data (column 6, line 67);

the buffer having a length equivalent to the block cipher size necessary to perform the cipher (column 6, lines 9-14);

decrypting the buffered segment of the received encrypted data to provide decrypted application data (column 7, lines 39-41);

forwarding the decrypted application data to a destination device (column 7, lines 4).

30. Jardin does not disclose buffering.

31. Lockhart discloses the use of a buffer (column 3, line 64 to column 4, line 17,).

Art Unit: 2131

32. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a buffer with an equivalent length to that necessary to perform a block cipher, since it has been held in the art (as illustrated by U.S. Patent Nos. 6,101,543 (column 10, lines 58-67) and 5,825,890 (column 17, lines 21-40) including additional data to a block cipher to make it the appropriate length improves the strength of the cipher.

33. Claims 6, 14, 15, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jardin in view of Lockhart as applied above, and further in view of U.S. Patent No. 6,052,785 to Lin et al., hereinafter Lin.

34. Regarding claims 6, 14, 15, and 20, Jardin and Lockhart do not teach after forwarding the decrypted unauthenticated application data to the server, notifying the client apparatus if a failure in authenticating the security record occurs.

35. Lin discloses after forwarding the decrypted unauthenticated application data to the server, notifying the client apparatus if a failure in authenticating the security record occurs (Figure 4 [blocks 418, 420], column 7, lines 25-41).

36. It would have been obvious to one of ordinary skill in the art at the time the invention was made to notify the client of a failure to authenticate, since Lin states at column 7, lines 19-24 that such a modification would allow a client to re-authenticate if their previous session and credentials had expired.

### ***Conclusion***

37. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2131

38. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

39. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

40. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

41. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 09/900,493


Art Unit: 2131

Christian LaForgia

Patent Examiner

Art Unit 2131

clf

 Page 11  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100